A Multifaceted Evaluation of the Reference Model of Information Assurance & Security

This is the authors' post-print version of the manuscript accepted for publication in Computers & Security.

Corresponding author: Dr. Yulia Cherdantseva

(CherdantsevaYV@cardiff.ac.uk)

DOI information: 10.1016/j.cose.2016.09.007.

Received at Editorial Office: 14 Jun 2016.

Article revised: 14 Sep 2016.

Accepted for publication on 20 Sep 2016.

A Multifaceted Evaluation of the Reference Model of Information Assurance & Security

Yulia Cherdantseva[1], Omer Rana, Wendy Ivins

School of Computer Science and Informatics, Cardiff University, UK;
email: y.v.cherdantseva,o.f.rana,ivinswk@cs.cardiff.ac.uk

Jeremy Hilton

Centre for Cyber Security and Information Systems, Cranfield University at the Defence Academy of the UK;
email: j.c.hilton@cranfield.ac.uk

Abstract

The evaluation of a conceptual model, which is an outcome of a qualitative research, is an arduous task due to the lack of a rigorous basis for evaluation. Overcoming this challenge, the paper at hand presents a detailed example of a multifaceted evaluation of a Reference Model of Information Assurance & Security (RMIAS), which summarises the knowledge acquired by the Information Assurance & Security community to date in one all-encompassing model. A combination of analytical and empirical evaluation methods is exploited to evaluate the RMIAS in a sustained way overcoming the limitations of separate methods. The RMIAS is analytically evaluated regarding the quality criteria of conceptual models and compared with existing models. Twenty-six semi-structured interviews with IAS experts are conducted to test the merit of the RMIAS. Three workshops and a case study are carried out to verify the practical value of the model. The paper discusses the evaluation methodology and evaluation results.

Keywords: Information Security, Information Assurance, conceptual model, reference model, analytical evaluation, empirical evaluation

[1]Corresponding author

Contents

1. Introduction

Evaluation is critical for any qualitative research claiming plausibility. The evaluation of a conceptual model, which is an outcome of a qualitative research, is an arduous task due to the lack of a rigorous basis for evaluation: "*a conceptual model exists only as a construction of the mind, and therefore quality cannot be as easily assessed*" [1]. Clear methods for the evaluation of conceptual models are still lacking and evaluation is often subjective and/or hard to formalise despite the fact that there are multiple proposals, originating both from research and practice, suggesting methods for the evaluation of the quality of conceptual models (at least fifty proposals are identified and analysed in [1]). Overcoming these challenges, in this paper, we present a concrete and detailed example of multifaceted evaluation of a Reference Model of Information Assurance & Security (RMIAS) [2, 3].

A reference model is a sub-type of a conceptual model, which strives to represent a problem at the industry level and to capture the entire domain knowledge [1]. Despite all discrepancies regarding the clear definition of the term reference model, it is generally accepted among academics that reference models are "*aggregated models, generic models, or theoretical models that have to be adapted to the specific conditions of enterprises and projects*" [4].

Information Assurance & Security (IAS), as with any other knowledge area, has either an explicit or assumed conceptual model, which describes the phenomenon being investigated, *"maps reality, guides research and systematizes knowledge"* [7]. Conceptual models convey the knowledge of IAS in a human-intelligible way and are usually graphically represented [8]. The pivotal purpose of a conceptual model is to facilitate understanding and communication among interested parties of the domain [1, p.244].

The importance of a conceptual model of the IAS domain is demonstrated via multiple implications. As often acknowledged, many security issues are caused by incorrect security decisions being taken on the basis of incomplete knowledge or misunderstanding of the security domain: threats, security goals and available

countermeasures [9]. In order to overcome this issue, the main entities of the knowledge area as well as the relationship between them should be defined and brought together in a conceptual model. A conceptual model of the IAS domain structures the acquired body of knowledge, creates a common ground for Information Security and Information Assurance professionals, and serves as a conceptual framework and a theoretical background for the researchers. A model clearly visualises the IAS domain, and enables newcomers to get a quick appreciation of its diverse and complex nature. A reference model of IAS plays a crucial role in the context of the information system development as it serves as a blueprint for the design of a *secure* information system. It provides a basis for the elicitation of system security requirements and for the development of an Information Security Policy Document (ISPD) [11, Sec.5].

IAS is a constantly developing domain, which changes shape following the evolution of society, business needs and ICT. Many studies highlight continual changes of IAS [13, 14, 15, 10, 16]. A conceptual model of a discipline often becomes debatable and requires a revision when the area of knowledge evolves and broadens [7]. As a result, the conceptual model of IAS is regularly revised reflecting the changes in the domain [16, p.228].

The broadening of the scope of IAS and its multi-disciplinary nature led to the growth of a number of experts who should be involved in the discussion of IAS. The knowledge of experts with different, often non-technical, backgrounds which relates to the various aspects of IAS such as legislation, human-factor, economy, administration, etc. should be captured in order to produce an holistic picture of IAS in an organisation. A group of experts discussing IAS issues may include, but is not limited to business experts (manager or business owner), IAS officers, computer and network experts (system administrators), legal advisers and Human Resources (HR-)experts. Hence, the model of the IAS domain should be expressed at the level accessible to this broad audience and should aid in engaging non-technical and non-security experts in security discussion and decision-making.

The RMIAS, which we discuss in greater detail in Section 3, is one of the

recent reference model of the IAS domain. It summarises the knowledge acquired by the IAS community of academics and practitioners to date in one all-encompassing model. It presents the key concepts of IAS and the interrelationships between them at a high level of abstraction in a form suitable for a wide range of experts with different backgrounds. The RMIAS approaches IAS holistically as a complex multi-disciplinary issue. The RMIAS was developed based on the analysis of the existing conceptual models described in Section 2 and on the extensive analysis of IAS literature summarised in [6]. The RMIAS was originally presented in [2] with a detailed description available in [3].

The ultimate aim of this research is to verify the following hypothesis:

The RMIAS provides more complete and accurate representation of the IAS domain, than the existing conceptual models of the IAS domain. The RMIAS reflects how the IAS domain is understood by IAS domain experts. It represents the domain in the form accessible by the experts with the different backgrounds and with the different levels of experience in IAS. Due to the above, the RMIAS helps to build a congruent understanding of the IAS domain in a multidisciplinary team of experts.

Summing up, our intention is to test whether the RMIAS corresponds with the vision of IAS possessed by the experts of this domain and whether the RMIAS meets the quality criteria of a conceptual model.

The remainder of the paper is organised as follows. In Section 2, we discuss the related literature. Section 3 provides the reader with the descriptions of the RMIAS. Next, in Section 4 we outline the evaluation methodology and justify the choice of the evaluation criteria. Then, Section 5 analytically evaluates the RMIAS and analyses the responses of the interviewees. Sections 6 and 7 contain the description of the arrangement and the feedback from the workshops and the case study respectively. Sections 8 discusses the evaluation results and the limitations of the evaluation methodology. Finally, in Section 9 we draw concluding remarks.

2. Related Work

In order to identify related work, we conducted a systematic review of the proposed models and frameworks of IAS following the methodology used in [19] for the analysis of security ontologies. The search was conducted in the following sources: Google Scholar, ACM Digital Library, IEEE Xplore Digital Library, SCOPUS.

Initially, 52 proposals were selected based on the title, keywords and abstract. The papers were examined and out of them closely related proposals were selected according to the following criteria:

- A model describes the IAS domain. Maturity models were excluded from the analysis because rather than describing the domain, they describe various stages of the Information Security (InfoSec) maturity of an organisation;
- A model addresses the IAS domain in general at a high level of abstraction. Two domain-specific models (e.g. models for governments and e-business) were also selected as they exploited a comprehensive approach to IAS;
- A model/framework has a visual representation (although the absence of a visual representation alone was not a reason for exclusion);

Finally, seventeen models and frameworks of IAS were selected for the analysis. Tables 1 and 2 summarise the analysis of the selected for review models. Table 1 gives an overview of the models and outlines (1) the basis for the development of a model, (2) model evaluation methods used, if any, (3) the presence of a visual representation, and (4) the purpose and contribution of a model. Table 2 shows a range of security concepts included in each model. Both tables include the RMIAS as the last row for the comparative analysis. The detailed overview and analysis of the examined models could be found in [3].

Table 1: The overview of the conceptual models of InfoSec and IA

Author (title), ref., year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
The CIA-traid [32] 1975 - 1987	Summary of the practical knowledge	No, but wide adoption in practice	Multiple versions could be found online	To convey the overarching goals of InfoSec to business and engineering management in a simplified way
McCumber [12] 1991	Practical experience of developer(s)	Brief application example, wide adoption in practice, it is also a part of the National Training Standard for Information Systems Security Professionals (CNSS 4011)	Yes, cube (three dimensions)	To function as an assessment and development framework, to identify and mitigate system vulnerabilities.
Parker [16] 1998	Practical experience of developer(s)	Analytical evaluation by the author using real life scenarios of information loss, mapping with InfoSec standards	No (set of goals)	An extended set of security goals which replaces the CIA-triad as a model of InfoSec, helps to prevent overlooking of threats
Maconachy et al. [26] 2001	McCumber's Cube updated to incorporated the notion of IA and the concept of defence-in-depth	Brief model application example, accepted as a model of IAS by the fifteen U.S. undergraduate IT programs	Yes, cube (three dimensions) and Time	A framework for teachers, students and analysts who are dealing with IA, which promotes a multidimensional view required to implement robust IA programs"
Vermeulen and Von Solms [24] 2002	Practical experience of developer(s) and literature analysis	Software tool supporting the framework is presented, but its correct functioning is not verified	Yes	A framework, methodology and a software tool for InfoSec management

Continued on the next page

Table 1 – *Continued from the previous page*

Author (title) [ref.] Year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
Trček [27] 2003	Experience of establishing health care information system infrastructure	No	Yes, cube (three dimensions)	To provide practitioners with steps and background to build optimal and balanced InfoSec solutions
Saint-Germain [28] 2005	ISO/IEC 17799	No	Yes, pyramid	Summarises a set of best practices and controls required to achieve information confidentiality, availability, and integrity
Lü [31] 2006	Critical analysis of other models	Brief model application example	Yes, cube (three dimensions) and time	To develop an IA plan and baseline strategies, to calculate costs of an IA architecture for large-scale information systems"
Jonsson [33] 2006	Analysis of the existing models of security and integrated models	No	Yes, system input and output	Security of a system presented in the context of its environment and is expressed in terms of input and output, assistance with reasoning about security
BMIS [10] 2008	Adopted from the University of Southern California (USA)	Case study	Yes, 3D pyramid	Promotes a holistic, dynamic, business-oriented approach to InfoSec in the networked environment, exploits system thinking to structure InfoSec
Dark and Harter [29] 2008	Not specified	No	No	A framework for teaching information security ethics
Al-Hamdani [30] 2009	Synthesis of other models	No	No	Supports a diligence-based approach to InfoSec based on the use of standards to enforce InfoSec program

Continued on the next page

Table 1 – *Continued from the previous page*

Author (title) [ref.] Year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
Ransbotham and Mitra [22] 2009	Observations of practice, interviews with experts, reviews of discussion groups, reviews of security guidelines and best practices, and analysis of existing models of crime	Empirical evaluation using alert data from intrusion detection devices	Yes	Development of empirical constructs and evaluation of their nomological validity, identification of more effective countermeasures
Parker [34] 2010	Practical experience of developer(s) and analysis of security polices of various organisations	No	Yes	To conduct vulnerability and threat analyses, security architecture revisions, selections and improvements of controls and practices, and their justification and prioritisation for implementation
Sabbari and Alipour [20]2011	Analysis of other models and standards for securing web services	Analytical Evaluation - Mapping to standards	Yes	Provides a mapping between areas of SOA and security requirements valid in each area
Kumar [25] 2011	Practical experience of developer(s)	No	Yes	To assist the IS manager with establishing an InfoSec management programs in governments
Oracle Architecture [21] 2011	InfoSec standards	Analytical validation against criteria derived from InfoSec standards	Yes	Summarises the layers of protection that are required in order to build an end-to-end organisation-wide InfoSec architecture

Continued on the next page

Table 1 – *Continued from the previous page*

Author (title) [ref.] Year	Basis for development	Evaluation	Visual Representation	Purpose(s) and Contribution
RMIAS [2] 2013	InfoSec and IA standards, academic and industry publications, security policies, survey of practitioners, informal interview and discussions with practitioners, detailed analysis of the existing IAS conceptual models and frameworks	Analytical evaluation against quality criteria for conceptual models; Empirical evaluation via interviews with IAS experts, case-study and workshops with MSc students	Yes	The synthesis of the existing IAS knowledge in a form accessible to a wide target audience including non-technical and non-security experts

Each analysed model has its purpose as Table 1 shows. Undoubtedly, this along with the perspective and experience of the model developer(s) affects the model scope (e.g. what elements it embraces). However, there is an aspect that unifies the examined models - all analysed models are destined for, first of all, conveying security knowledge to a wide non-security audience and the target audience typically includes business experts and managers. Also, the majority of the analysed models attempt to cover the full breadth of the IAS domain [10, 34, 12, 16, 26, 24, 28, 30, 31, 32, 33] rather than a specific facet of it. In general, only the examination of the different facets of IAS and approaching it from different perspectives allows building a "*complete picture*" of the domain.

We shall now discuss how well the authors of the examined models inform the readers as to how their models were developed. Parker's model [16] is underpinned by 28 years experience of the author in computer crime and security research. The narrative of the model is rich with real life cases and examples from the author's personal professional experience. Ransbotham and Mitra [22] in detail describe the development process of the Information Security Compromise Process (ISCP) model. The model is draws upon the examination of four sources of information: (1) the observations of the operations of managed security service provider data centres, (2) interviews with 30 information security experts, (3) analysis of discussions in relevant online groups for understanding motivation for attacks, (4) analysis of security-related guidelines and best practices. The principles of grounded theory were followed

Table 2: Concepts represented in the analysed models of InfoSec and IA

Author (title) [ref.]	Security Goal	Technical Countermeasures	Organisational Countermeasures	Human-oriented Countermeasures	Legal Countermeasures	Other Categorisation of Countermeasures	Information/Information State	Time/SDLC	Threats/Attacks	Vulnerabilities	Cost/Budget/Asset	Physical Infrastructure	System and Environment	Actors/Users	Characteristics of organisation	Information Sensitivity, Form, Location	IAS drivers
The CIA-triad [32]	X																
McCumber [12]	X	X	X	X			X										
Parker [16]	X																
Maconachy et al. [26]	X	X	X	X			X	X									
Vermeulen and Von Solms [24]	X		X			X		X									
Trček [27]		X	X	X	X						Asset						
Saint-Germain [28]		X	X		X	X											
Lü [31]		X	X	X		X		X			Cost						
Jonsson [33]	X	X							X	X			X	X			
BMIS [10]		X	X	X		X											
Dark and Harter [29]		X	X	X	X												
Al-Hamdani [30]	X	X	X	X		X			X								
Ransbotham and Mitra [22]		X	X			X			X	X					X		
Parker [34]	X	X	X	X		X			X								
Sabbari and Alipour [20]	X	X	X	X								X					
Kumar [25]		X	X	X		X		One stage			Budget						
Oracle [21]		X	X				X								X		
RMIAS [2]	X	X	X	X	X		X	X								X	X

to justify the validity of the ISCP model.

For the RMIAS [3], the development method along with the range of the literature examined is thoroughly documented. The RMIAS was developed following the Best-Evidence Synthesis approach [23]. In [3], the set of criteria is developed based on which the dimension were included in the RMIAS. The aspects of IAS, which are not (or, at least, not explicitly) included in the RMIAS, are also discussed and the vindication of non-inclusion is given. In the RMIAS, also a literature search methodology used to identify relevant reference models is also presented.

Apart from Ransbotham and Mitra [22], for the majority of the analysed models, authors do not describe the methodology, or scientific principles they followed while developing their models, and rarely discuss in detail the literature examined in order to create a model, but present such analysis in a patchy limited manner. At best, it is stated that a model is based

upon the analysis of InfoSec standards and the standards are named as in [21, 24], or upon the analysis of existing models of security [20, 33, 30], but the analysis of the standards and model is typically not presented. In [10, p.7], for example, other existing models are criticised as simplistic, static and not being able to deal with the changes within an enterprise and the culture adaptability, but the models this criticisms is addressed to are not named. Due to the sparse documentation of the development process and of the basis for the model development, newly proposed conceptual models of IAS are often seem to be only loosely grounded in existing knowledge, and do no provide any means for linking or comparing the new model with the existing ones.

Next, we shall discuss how the examined models are evaluated. According to Table 1, eight out of seventeen analysed models are not accompanied by any kind of evaluation. It must be noted here, that in Table 1 we discuss how the model is evaluated in the original publication and then state if any other evaluation exisits we are aware of. Despite the absence of formally described evaluation, or the evaluation only through a brief simplified application example, the models such as the CIA-triad, McCumber's Cube [12] and Maconachy et al. model [26] are widely adopted in practice, and even are included in a security standard or training materials (Table 1). This could be regarded as an acceptance and a positive evaluation by the IAS community.

The following models [34, 16, 12, 24, 25] draw upon the practical experience of the model developer(s). Empirically developed models provide value to the domain, however, according to the scientific principles of qualitative research they require further unbiased evaluation. Parker [16], who suggested the conceptual model of InfoSec which embraces six security characteristics - Confidentiality, Possession or Control, Integrity, Authenticity, Availability, and Utility (also known as Parkerian Hexad), - in order to demonstrate the validity of his model uses information loss scenarios. Real life cases are discussed along each of six security characteristics. In [24], the authors develop a tool to support the proposed framework, but the validation of the tool is not presented. It is not verified in any way, whether the tool produces valid useful results.

Table 1 shows that only three examined models ([16, 20, 21]) are accompanied by analytical evaluation and only one model [22] is empirically evaluated. Three models are mapped against InfoSec guidelines and standards. Sabbari and Alipour [20] examine security standards published by OASIS, W3C and the Liberty Alliance for Web Services. The Oracle InfoSec conceptual architecture [21] refers to ISO 27001, NIST, the International Information System Security Certification Consortium (ISC2), Cloud Security Alliance (CSA) and European Union Agency for Network and Information Security (ENISA) security standards. Parker [16] maps his hexad onto security standards and best practices such as BSI BS 7799: 1995 *Code of Practice for Information Security Management* and COBIT as well as compares his understanding of InfoSec with that of Neumann [17]. The model proposed by Ransbotham

and Mitra [22] is empirically evaluated using alert data from intrusion detection devices.

Only in one out of examined models the number of people involved in the development or evaluation is stated. In [22], 30 information security experts were interviewed, however, the details of the interview process and full transcripts, as well as the profiles of the interviewees are not available to the reader.

In the examined literature, we did not encounter models which were thoroughly evaluated using both empirical and analytical evaluation, and a multi-criteria approach. Often, the conceptual models of IAS are presented in the format of a position paper and are not substantiated by any evaluation. Analytical evaluation via comparison with other existing model is typically absent in the examined publications. The models specifically designed for communication purposes and specifically targeted at a non-technical audience are not tested for their accessibility to the target audience, or the ease to understand and use. Overall, the involvement of people other than the model developer(s) in the evaluation of models is limited. In this research, we aim to remedy the drawbacks found in the existing literature with regard to the evaluation of conceptual model of the IAS domain.

Finally, it must be notated that the type of publications examined vary between a conference papers ([30, 26, 31]), a book ([16]) and a white paper ([21]). Understandably, it is very difficult to present in one, even a journal paper, not to mention a conference paper with a highly restricted page count, both the model itself and its sound evaluation. Hence, the author(s) of a conceptual model for presenting the model and its evaluation should either (1) consider such publication formats as a book, thesis or white paper, or (2) publish a series of follow-up papers.

3. RMIAS and its Use

The true novelty of the RMIAS is in bringing together the segregated, discrete knowledge of the IAS domain in a form suitable for a wide range of experts with different technical, non-technical, security and non-security backgrounds.

The RMIAS, which is depicted in Figure 1, has four dimensions (while covering the key concepts of IAS, four dimensions of the RMIAS do not overlap and do not duplicate each other):

- **Security Development Life Cycle Dimension** (top left quadrant) illustrates the progression of IAS along the Information System Development Life Cycle (ISDLC);
- **Information Taxonomy Dimension** (top right quadrant) outlines the characteristics of information being protected;
- **Security Goals Dimension** (bottom right quadrant) outlines the set of eight security goals, also referred to as the IAS-octave, which includes Confidentiality, Integrity, Avail-

ability, Accountability, Auditability, Authenticity & Trustworthiness, Non-repudiation, and Privacy.

- **Security Countermeasures Dimension** (bottom left quadrant) categorises security countermeasures.

The RMIAS is a generic abstraction. Before its use in the context of a specific organisation the following elements of the RMIAS should be adapted:

1. The generic security development life cycle should be replaced with the one specific to the organisation; and
2. The information taxonomy should be extended with the information sensitivity classifications and the location classification which are specific to the organisation.

In addition to the descriptive knowledge described above, the RMIAS also embeds the methodological knowledge[3]. Further this sections explains how the RMIAS may assist with the development of an Information Security Policy Document (ISPD). There is a hierarchy of security policies, where each policy document covers security at a different level of detail [36]. In this paper, an ISPD refers to a governing policy document which specifies what security goals should be achieved and what security countermeasures should be put in place at a high level of abstraction leaving more precise details for the supporting documents (e.g. technical policies, job aids and guidances) [21, 36]. The detailed description of an ISPD and its content is given in ISO/IEC 27002:2005, Sec 5.1 [11].

An ISPD consists of a number of statements[4], e.g. *"to ensure integrity and confidentiality, all backup data must be encrypted"*. A security policy statement does not typically provide the full details (e.g. what software or hardware should be used to encrypt data or who is the person responsible for signing permissions for taking documents out) [36]. This level of abstraction is sufficient for and accessible by the target audience of the RMIAS (i.e. when discussing IAS issues a multi-disciplinary team does not typically require to know about encryption algorithms or the in-depth details of a legal agreement with a third party and the like; these details may be dealt with by a domain expert).

[2]The security countermeasures dimension outlines only some countermeasures related to each type, but not the exhaustive lists. Within the information taxonomy dimension, attributes *location* and *sensitivity* possess values specific to an organisation.

[3]The descriptive knowledge - "*knowledge that*" - accumulates assertions about the world, while the methodological knowledge - "*knowledge how*" - outlines instructions for conducting actions [35]

[4]In the context of InfoSec management the term "information security policy statement" is usually used. In the system engineering context the similar type of statements is often referred to as system or security requirements.

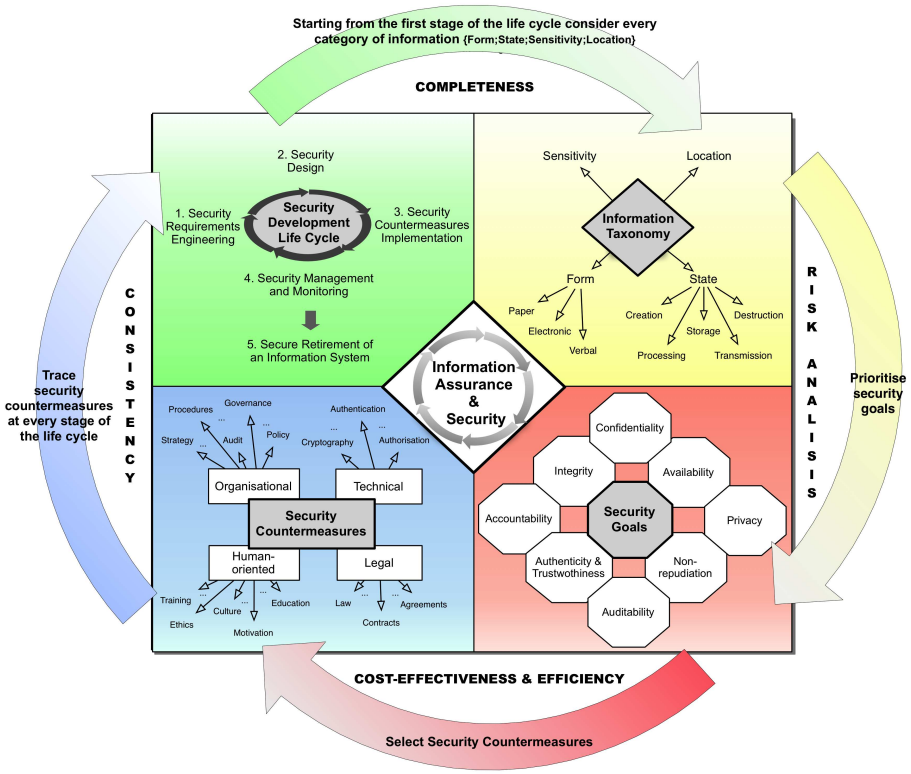

Figure 1: The Reference Model of Information Assurance & Security (RMIAS)[2]

In the RMIAS, an element of one dimension must be combined with an element of each other dimension in order to create a comprehensive list of situations in which information needs protection. Then, a policy statement is created for every combination. This method ensures that a security policy statement exists for every possible risk situation.

We demonstrate the use of the RMIAS for the development of an ISPD on the example of a Small and Medium-size Enterprise (SME) *Translate*. *Translate* is a small 15-person translation business established in 1993 which offers a wide range of translation services to large and small businesses, and individuals. *Translate* classifies its information into Public, Proprietary, Restricted Sharing and Confidential. Locations are categorised as follows: *controlled* - the company's offices, *partially controlled* - the supporting IT company and third parties storing information on behalf of Translate and home environment (employees who work from home); and *uncontrolled* - locations other than the above.

First, the RMIAS is adapted for the specifics of *Translate*. In the Information Taxonomy dimension, the location and sensitivity classifications which are in use by Translate are added to the RMIAS. Information of all three forms is dealt with by Translate and, therefore, all three forms are kept in the model. Translate adopted the IAS-octave as a set of security goals. At this stage, the elements of the three dimensions - Information Taxonomy, Security Goals and Security Countermeasures - are combined to produce an ISPD. In terms of the life cycle, Translate is at the requirements engineering stage.

The format of a table provides a convenient way for combining the elements of the three dimensions of the RMIAS. Table 3 has six columns: form, sensitivity, location, state, security goal and security countermeasure type & description. The table is populated with all possible combinations of values of the following attributes: form, sensitivity, location, state and security goal. At this stage, the last column - security countermeasure type & description - is left empty.

The number of all possible combinations of the categories of information and security goals (which is also the number of rows in the table) is calculated as follows:

$$N = N_f * N_s * N_{sen} * N_l * N_{SG}, \tag{1}$$

where

- N - the number of possible combinations of the categories of information and security goals,
- N_f - the number of the forms of information,
- N_s - the number of the states of information,
- N_{sen} - the number of the levels of information sensitivity,
- N_l - the number of locations, and
- N_{SG} - the number of security goals.

Table 3: The development of an Information Security Policy Document for Translate using the RMIAS

	1. Form	**2. Sensitivity**	**3. Location**	**4. State**	**5. Security Goal**	**6. Security Countermeasure Type: Description**
1	Paper	Public	Uncontrolled	Processing	Privacy	Not required.
2	Electronic	Public	Controlled	Storage	Non-repudiation	Not required.
3	Electronic	Public	Controlled	Storage	Availability	Technical: All electronic information must be backed up every night (Backup on an external hard drive and using an online backup service).
4	Paper	Confidential	Controlled	Storage	Confidentiality	Organisational: Store in a safe and ensure that only authorised personnel have access to the safe.
5	Paper	Confidential	Uncontrolled	Transmission	Confidentiality	Organisational: Documents must not be taken out of the office.
6	Paper	Proprietary	Controlled	Processing	Accountability	Organisational: Access to all proprietary documents must be logged. Legal: Non-disclosure agreement must be sighed by all members of staff granted access to proprietary information.

Each row (i.e. each combination of a category of information and a security goal) in the populated table refers to a particular scenario or rather a group of scenarios in which the information of that category may need protection from threats covered by the referenced security goal.

For example, row 1 in Table 3 refers to privacy of paper documents which are classified as *Public* and processed in an uncontrolled environment (e.g. an advertisement brochure is read by a prospective client). Row 2 refers to the non-repudiation of information which is contained in electronic documents classified as *Public* and stored in a controlled environment (e.g. a video-press release of Translate which is stored on the company's server).

Next, we consider each row in the table and establish how critical the security goal is for the category of information. If Translate decides that the violation scenarios outlined by the row are realistic and pose threat to the organisation then actions should be taken to achieve the security goal for the category of information. A decision is then made on which security countermeasures must be put in place for the prevention of the scenario. A multi-disciplinary team of experts may be involved in this discussion.

The number of possible combinations of information categories and security goals, as calculated according to the formula above may be substantial. However, not each possible combination (row in the table) is applicable in the context of a specific organisation. Consequently, security countermeasures and, as a result, security statements in an ISPD are required not for every combination. Nevertheless, it is critical to identify (and keep them in the table) all potential situations in which information needs protection, and then consciously mark irrelevant ones as such. It ensures that no potential security violations is overlooked, and enables the traceability and defensibility of security decisions.

In row 1 of Table 3, no security countermeasures are required to protect privacy of a *Public* document as there are no such scenarios in which privacy may be violated by misusing a *Public* document. Hence, for this combination no security policy statement is developed. Similarly, in row 2, the non-repudiation of a *Public* document poses no threats to Translate and this combination of attributes and the security goal is excluded from further consideration. However, while non-repudiation is not critical for a *Public* electronic document located in a controlled environment, availability is. The scenarios in which the availability of a *Public* electronic document located in a controlled environment may be breached may be as follows: (1) an employee deletes the document by mistake, (2) the physical damage of the server on which the document is stored (e.g. due to fire or flood), (3) the external host of the document does not provide access to the document in violation of a service agreement, etc. Row 3 specifies that the availability of the electronic documents, which are classified as *Public* and stored in a controlled location, must be ensured by means of creating backups both on an external hard drive and in the cloud using one of online backup services.

Row 4 contains a security policy statement which dictates that for the *Confidential* paper

documents which are stored in a controlled location (e.g. printed financial and audit reports stored in Translate's office) an organisational security countermeasures should be put in place, namely, the documents must be stored in a locked safe and it must be ensured that only authorised personnel have access to the safe. Row 5 declares that *Confidential* paper documents cannot be transmitted to an uncontrolled environment.

Row 6 refers to the accountability for the use/misuse of information classified as proprietary while it is being processed in the paper form in a controlled location. To achieve accountability the access to *Proprietary* paper documents must be logged (organisational security countermeasure) and non-disclosure agreements must be in place with every employee of Translate who has access to the information classified as *Proprietary* (legal security countermeasure).

4. Evaluation Methodology and Criteria

A conceptual model may be evaluated analytically or empirically [38, 39]. While empirical evaluation involves prospective users of a model or modelling language, analytical evaluation does not. Analytical evaluation is conducted by an evaluator/researcher(s) usually with the exploitation of an evaluation framework and based on the examination of available information about the evaluated object. Both types of evaluation have their advantages and disadvantages.

One of the advantages of analytical evaluation is that it is usually performed by experienced individuals, who have extensive knowledge of a evaluated object and of an evaluation technique. Evaluators are well motivated and dedicated to evaluation and analysis. An analytical evaluation allows considering an object in greater depth since it is less restricted in terms of time and cost than empirical evaluation. The time and cost of analytical evaluation is lower because it does not require a large number of people to be involved and motivated [40]. Analytical evaluation is often conducted by the model developer(s), who are inevitably biased. The evaluation results are influenced by the perspective and background of model evaluator(s). In research projects, a decision to give preference to an analytical evaluation is often dictated by time and budget restrictions.

The merit of a method embedded into a conceptual model or of a modelling technique could only be realised if it is effective in practice. A method ("knowledge how") as opposed to a thesis ("knowledge that") is not either true or false, but is either effective or not [41]. Where analytical evaluation could only make predictions about the effectiveness of a method and its potential adoption in practice, an empirical evaluation may refute or corroborate results of analytical evaluation as well as predictions from theories [42].

In addition to a higher cost and difficulties in administration, in comparison with analytical evaluation, empirical evaluation suffers from other drawbacks. A low motivation of participants and a danger of the misunderstanding of an evaluated model or method by participants are only some of them. Participants are also often affected by additional factors that

may not always be accounted for by research (e.g. mood, language understanding, attitude to an experiment). Furthermore, several empirical studies with a significant number of participants should be conducted and the results should be repeated before any conclusion may be taken as final.

Since both evaluation approaches - analytical and empirical - have their limitations [43], a combination of different evaluation methods was exploited to overcome the limitations of separate methods. A evaluation route which includes different types of evaluation was designed and pursued in order to test the hypothesis declared in Section 1 and to demonstrate the merits of the RMIAS in a valid sustainable way.

The evaluation of the RMIAS is intended to verify both the scientific value and pragmatic value of the RMIAS by combining the following methods of evaluation:

- To test the scientific value:
  (1) *Grounding in the existing literature;*
  (2) *Analytical evaluation by the model developer;*
  (3) *Interviews with academic and industry IAS experts;*
- To test the practical value (utility):
  (4) *Workshops with MSc students and IAS practitioners;* and
  (5) *Case study.*

Figure 2 schematically depicts the RMIAS evaluation methodology (the evaluation criteria outlined Figure 2 are discussed and defined later in this section).

The scientific value (truthfulness) of the RMIAS is, at least to some degree, justified by the IAS literature it draws upon. As manifested by the analysis presented in [3, Chap.3], there are research and/or industry publications related to each element of the RMIAS.

Since this justification is not deemed to be sufficient, to prove the scientific value of the RMIAS further, the model is evaluated analytically by the model developer for its compliance with the quality criteria of conceptual models. This criteria are introduced further in this section. In Section 5, the RMIAS is also compared with other IAS conceptual models and it is analytically demonstrated that the RMIAS outweighs the other models in terms of completeness and accuracy. The developer possesses the in-depth understanding of the model and is well equipped to perform analytical evaluation. However, such evaluation is subjective because the developer is inevitably inclined towards her proposal. Furthermore, the evaluation results are unavoidably affected by the perspective and background of the evaluator.

In order to complement and deal with the limitations of the analytical evaluation mentioned above, a series of semi-structured interviews[5] with IAS experts, who are impartial

[5]Semi-structured interview is an interview, run by a researcher, where there is a script

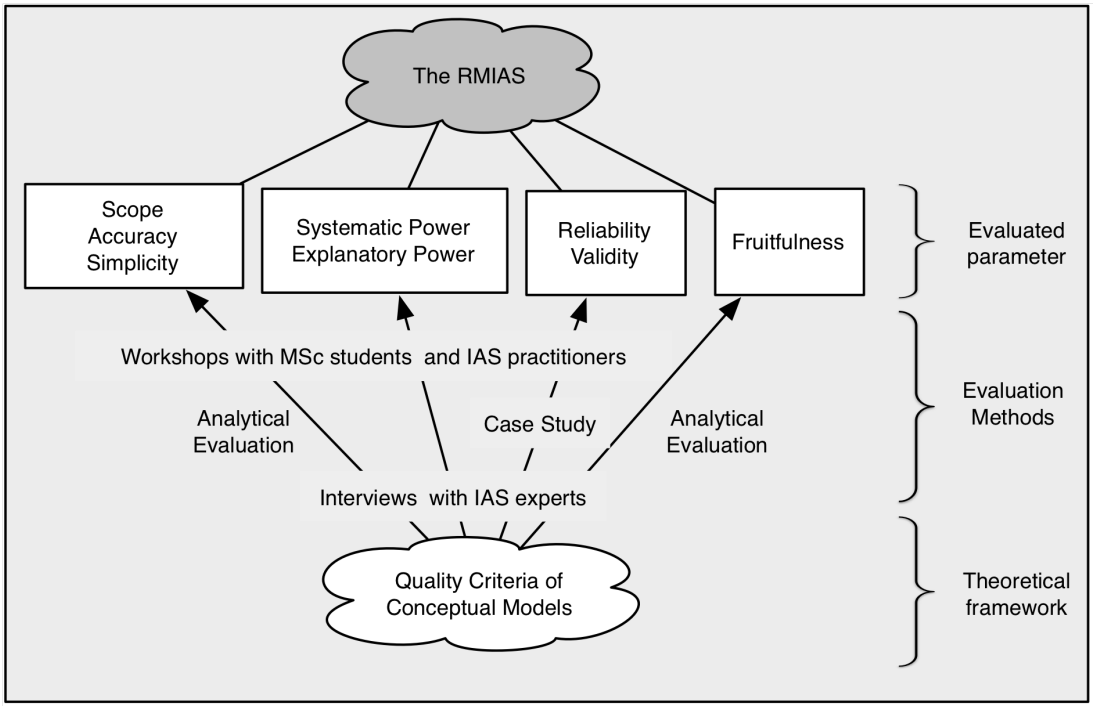

Figure 2: The evaluation methodology

towards the model, was conducted to apprise the quality of the RMIAS. The interviews aimed to test how well the RMIAS corresponds with the experts' understanding of the IAS domain and how well it complies with the quality criteria of conceptual models, according to the opinion of the experts. Testing the hypothesis, it was also examined whether the RMIAS represents the domain in the form accessible by the experts with the different backgrounds and with the different levels of experience in IAS.

For the validation of the methodological knowledge of the RMIAS it was essential to empirically demonstrate the practical value of the model [44]. The practical value of the RMIAS (i.e. how viable and useful the model is in practice) was tested via the workshops with MSc students and IAS practitioners and via a case study.

Many evaluation frameworks agree on the need for a multi-criteria approach. For the evaluation of the RMIAS we adopted the criteria which are suggested in [7] and further elaborated in [38]:

1. **Simplicity** - among models, equal in other ways, preference is given to the simpler model;
2. **Accuracy** - a model as well as the concepts it incorporates should be accurate and explicit;
3. **Scope** - a model should cover the broader scope of a modelled domain and should not overlook essential concepts;
4. **Systematic power** - a model should help to organise concepts and relationships between them in a meaningful systematic way;
5. **Explanatory power** - a model should assist with explaining and predicting a phenomena;
6. **Reliability** - a model should be valid (applicable) in all situations for which it is designed (in our case, we interpret it so that the model should be applicable to a wide range of organisations) and should lead to a similar understanding when applied to the same phenomenon by different users;
7. **Validity** - a model should provide valid representations and findings; and
8. **Fruitfulness** - desirably a model should suggest research problems and hypotheses for testing.

The choice of these evaluation criteria is driven by the following considerations:

- Purpose: These criteria are specifically destined for the evaluation of a conceptual model of an area of research (i.e. a reference model).

---

which covers some questions and helps to keep the focus of the discussion, but there is still a room for openness, flexibility and improvisation [43].

- Application: These criteria are applied to the evaluation of information seeking and retrieval research by the authors of the criteria [7]. The criteria are also exploited for the evaluation of a definition of an IS [38], independently of the authors of the criteria. Other evaluation frameworks present only a theoretical basis, but do not provide any application examples.
- Completeness: The set of quality criteria is more comprehensive than the sets of the quality characteristics found in other proposals.

The RMIAS was analytically evaluated against these eight criteria by the model developers and by the IAS experts interviewed. The workshops and case study contributed to the evaluation of the RMIAS with regard to reliability and validity.

5. Analytical Evaluation and Analysis of the Interviews

Section 5.1 provides the details of the interviewing process according to the rules outlined in [43].

Sections 5.2 - 5.9 present the discussions on how the RMIAS addresses each of the eight chosen quality criteria. The first part of sections 5.2 - 5.9 outlines the comments of the authors related to a particular criteria - analytical evaluation and comparison with other models. The second part of Sections 5.2 - 5.9 discusses the comments of the interviewed experts.

The comparison with other models is supported by Table 2 which shows a range of security concepts included in each model.

5.1. Arrangement of the Interviews

For the interviews, the professionals and academics who have experience in the IAS domain or related areas were targeted. Twenty six experts who participated in the evaluation, first, were given a presentation which briefly discussed the existing models of IAS and described the RMIAS in detail. Then, the participants challenged the model in a question and answer session. Three out of five presentations were followed by a workshop , where the participants used the RMIAS for the ISPD development.

The interviews were arranged either on the same day following the presentations or, in several cases, at a later date. Each interview lasted between 30 - 60 minutes. At the beginning of an interview, the purpose of an interview was communicated to an interviewee and reassurance was given that in all written work the responses will appear anonymously. The participants were also presented with the definition of evaluation criteria as adopted from [7] and [38], and summarised in Section 4.

To facilitate the interviews, a questionnaire was developed based on the chosen set of evaluation criteria. For each criterion a number of questions was developed. A pilot test of the questionnaire was run with a group of three PhD students and two lecturers, who

specialise in InfoSec and Privacy, at the School of Computer Science & Informatics, Cardiff University. The group was familiar with the RMIAS and informed about the objectives of the study. The questionnaire was corrected to enhance its clarity and several questions were dropped as monotonous as a result of the comments of the pilot-test group.

The final version of the questionnaire included fifteen questions. The full version of the questionnaire could be found in [3, App. 10]. First three questions gathered information about a respondent (the number of years of experience, nature and area of expertise). The remaining questions asked a respondent to evaluate the RMIAS in terms of the chosen quality criteria. The last two questions in the questionnaire related to the fruitfulness of the RMIAS for research. These questions required a respondent to have an academic background in IAS.

The interviews were semi-structured. The questionnaire provided a template for the discussion, but the participants were invited to give extended answers and to explain their position. At the end, the respondents were invited to provide any comments that were not captured by the questions. Both the transcripts and notes were used as the recording technique. All presentations, interviews, workshop and the analysis of the results were carried out by the authors. With seven interviewees the interviewer was acquainted as with colleagues prior to the presentation and interviewing procedure, and two of seven interviewees were exposed to the early versions of the RMIAS and knew the details of the development process. Other interviewees the interviewer had not previously met.

Overall, 26 full responses were received over the period between November 2012 and April 2013. The experience of the respondents varies from 1 to 32 years with the average of 9.9 years. Among the interviewees there were 5 academics, 15 practitioners and 6 experts whose experience comes from both research and practice. The respondents specialise in the diverse range of the aspects of IAS and in related domains, including cyber security and defence, system modelling, requirement engineering, trusted computing, forensics etc. The profile of the interviewees, the detailed version of which could be found in [3], confirms that the RMIAS was evaluated by the independent experienced audience and that the RMIAS was approached from different perspectives conditioned by the backgrounds of the respondents.

The transcripts of interviews could be found in [3]. Due to the space limitations, in this paper we use thin description[6] of interview results while presenting the analysis of the interviews.

5.2. Simplicity of the RMIAS

Simplicity is a subjective characteristic: what is simple for one individual, may be complex for another. Objectively, simplicity may be analytically evaluated against other models. In

[6]While thick description means that verbatim quotations from responses are used, thin description refers to the use of little or no quotations [43].

comparison with other models (e.g. McCumber's cube [12], Maconachy et al. [26]), the RMIAS is more complex. The RMIAS has a wider scope than other models and, therefore, it inevitably has more elements and is less simple. However, according to the Ockham's razor principle, the simple explanation or model should only be preferred until simplicity can be traded for greater explanatory power. It may be hypothesised that the RMIAS has greater explanatory power than the other models because it may represent more security issues and solutions, and it also makes the interrelationships between the IAS concepts explicit. This statement is supported by Table 2 which shows that none other of the examined models covers the same range of security concepts as the RMIAS.

The RMIAS also attempts to cover the full breadth of the IAS domain. As the result of this, in the trade-off between simplicity and scope (completeness), in the RMIAS, the preference is given to the completeness.

Despite being more complex than other analysed models according to the analytical evaluation conducted by the authors, the RMIAS is considered as relatively simple and easy to grasp by the interviewed experts and even by newcomers to the IAS field as discussed in Section 6. In order to enhance its intelligibility, the RMIAS is duly accompanied by a narrative. The definitions of every element of the RMIAS are provided and the interrelationships between the elements are explained. The visual appearance also aims to improve the intelligibility of the RMIAS. During the workshops, the RMIAS was presented to the audience which had different levels of expertise in IAS. The feedback from the participants indicates that even the novices to IAS find the model simple and easy to understand. As discussed in Section 6, the novice participants along with more experienced ones successfully used the RMIAS for the development of an ISPD during the evaluation workshops.

In the interviews, there were two questions capturing the opinion of interviewees with regard to the simplicity of the RMIAS:

- Question 4 - Are the elements of the RMIAS simple?
- Question 5 - Are the relationships between the elements simple? (The relationships are illustrated by arrows.)

Twenty-two out of twenty-six interviewees described the elements of the RMIAS as simple. Although two respondents found the elements of the RMIAS simple, they suggested to change the layout and improve the visual effectiveness of the RMIAS. One respondent interprets the role of the security development life cycle in the RMIAS as it is intended, but suggests that the visual appearance of the RMIAS does not convey the view on the life cycle as a time line in the most effective way. In order to eliminate possible misinterpretations of the role of the security dimensions life cycle, the detailed explanation of the role of this dimension and of its interrelationships with other dimensions is presented in the narrative of the RMIAS in [3]. Another two respondent agreed that the elements of the RMIAS are simple, but had an opposite opinion regarding the simplicity of the implementation of the RMIAS. Four

respondents pointed out at the difficulty to understand the elements of the RMIAS.

Answering question 5, seventeen interviewees agreed that the interrelationships between the dimensions of the RMIAS are simple. Seven respondents did not see the interrelationships as simple, while the remaining two were not sure about the answer.

While only four interviewees did not find the element of the RMIAS simple, nine did not see the interrelationships as simple or were not sure about them. Overall, the interrelationships between the elements of the RMIAS pose more difficulties for understanding than the elements of the model.

The responses for questions 4 and 5 indicate that the majority of the interviewees found both the elements and interrelationships simple. However, in the future further research is required into the improvement of the visual appearance of the RMIAS and additional attention to the clarity of presentation/narrative of the interrelationships between the elements of the model.

5.3. Accuracy of the RMIAS

The comparison of the RMIAS with its predecessors demonstrates that the RMIAS is more accurate than other analysed models, since it includes a more detailed taxonomy of information and classification of security countermeasures, and embraces the broader set of security goals (Table 2). The RMIAS also contributes to accuracy by underscoring the distinction between security goals and security countermeasures, and by outlining the interrelationships between the concepts of IAS.

In the interviews, two questions were intended to capture the opinion of the respondents with regard to the accuracy of the RMIAS:

- Question 6 - Are the classifications included in the model accurate (the information taxonomy, the set of security goals and the types of security countermeasures)?
- Question 7 - Are the interrelationships between the elements of the model accurately described?

Answering question 6, eighteen out of twenty-six respondents agreed that the information taxonomy, the set of security goals and the classification of security countermeasures are accurate. Four respondents found other dimensions as accurate, but did not perceive the information taxonomy as accurate and suggested to extend it with, for example *the purpose of use* and *responsibility*.Three respondents did not to answer this question. One respondent although agreed with the accuracy of other classifications, noted that the nuance differences between some security goals are hard to see. Hence, overall only 5 responders perceived one of the dimensions of the model as inaccurate.

The additional elements suggested by the respondents such as responsibility and the purpose of use may be added to the Information Taxonomy of the RMIAS in the future. Regarding

the accuracy and completeness of the forms of information outlined in the RMIAS, the examined literature does not currently indicate the existence of any other form of information apart from paper, verbal and electronic forms which are captured in our model. However, we foresee that new forms or formats of information may appear in future. Information in paper form appeared in the early 2nd century AD, when the paper-making process was developed in China. Information in electronic form emerged with the invention of the first electronic devices. The advances of technology in future may give rise to new currently unknown forms of information. In this case, the Information Taxonomy of the RMIAS must be extended and newly emerging forms must be included in the model.

Fourteen respondents perceived the interrelationships between the dimensions in the RMIAS as accurate. Nine respondents perceived the interrelationships as inaccurate. Among those who did not see the interrelationships as accurately described, three respondents had doubt or suggested a clarification for the top arrow linking the security development life cycle and information taxonomy dimensions. Three respondents suggested the clarification for the arrow linking the security goals and security countermeasures dimensions, where the role of risk analysis and cost-effectiveness analysis shall be pointed out. Two respondents highlighted the inaccuracy of the link between the information taxonomy and security goals dimensions. Three respondents were not sure about their answers.

Overall, the accuracy of the RMIAS was evaluated by the respondents positively. Eighteen out of 26 respondents (69%) agreed with the accuracy of the elements of the model. As for the relationships between the dimensions, depicted by the arrows in Figure 1, while 14 respondents (54%) stated that all interrelationships are accurately described, 9 (34%) pointed out that one out of four arrows is not accurately described and further clarifications are needed.

5.4. Scope of the RMIAS

Scope covered (completeness) has a particular importance for the RMIAS. First, in order to convey the complexity and heterogeneity of IAS, the RMIAS must cover the full range of IAS concepts required by the target model of the RMIAS. Second, the RMIAS serves as the basis for the semantics of an IAS modelling notation in [3, 18]. The above two reasons make it critical to ensure that the RMIAS covers an adequate scope and that all key IAS concepts are covered by the model.

The key source that inspired the work on the RMIAS was McCumber's Cube [12], published in 1991, and its updated version - the model of Maconachy et al. [26] released in 2001. These models were included in security training and education programs in the US. The RMIAS builds upon these two models and extends them with new security concepts reflecting the ever-changing landscape of the IAS domain and responing to the call for a regular revision of a conceptual model of the IAS domain stated in [16, 34]. The RMIAS extends McCumber's Cube and the Machonachy et al. model in several ways: (1) it adds the legal security countermeasures and extended the scope of organisational and human-oriented countermeasures, (2)

it enriches the list of possible information states with two missing states, namely creation and destruction, (3) it enriches the model with the information about the interrelationships about the concepts of the IAS domain, and about the drivers that stipulate security decision-making. It is pointed out by well recognised security experts that the CIA-triad does not adequately reflect the contemporary state of IAS and requires an extension [16, 37]. Notably, the RMIAS addresses this call and extends the CIA-triad drawing upon the existing literature and other models analysed.

The greater scope of the RMIAS is demonstrated by means of benchmarking the RMIAS against other models. Table 2 confirms that none of the other models incorporates all four dimensions of the RMIAS. The same table shows that none of the other models considers such attributes of information as sensitivity, location and form. Only four models [26, 24, 31, 25] mention time or the ISDLC, but these models overlook other critical dimensions of IAS or types of security countermeasures. According to the same table, no other model apart from the RMIAS incorporates the drivers behind IAS decisions. The comparison with other models evidences that the RMIAS is more complete than any of the analysed models because the RMIAS (1) outlines an extensive list of security goals which is supported by the analysis, (2) incorporates the categorisation of security countermeasures which embraces all possible types of countermeasures at the high level of abstraction, and (3) includes the drivers underpinning IAS decisions. The wide scope of the RMIAS comes from adopting the broad view on an information system as a socio-technical system and from interpreting IAS as a complex multifaceted discipline, rather than a purely technical one.

In the interview, there were two questions related to the scope (completeness) of the RMIAS:

- Question 8 - Does the model include all elements/concepts essential for the IAS domain? If, in your opinion, there are some essential, but missing from the model elements/concepts, please, name them.
- Question 9 - Does the model include any elements that are not relevant to the IAS domain?

In question 8, eighteen out of twenty-six respondents confirmed that the RMIAS is complete and covers the appropriate for its purposes scope. Five respondents suggested to add new elements to the RMIAS such as collaborative aspect, risk analysis/assessment, user scenarios, additional emphasis on human factor, and business goals.

The uncertainty regarding the completeness of the RMIAS expressed by the participants is expected. A complex domain such as IAS may be approached from various perspectives which would focus on different elements of the domain. The elements, which the respondents suggested to include in the RMIAS, are already covered by the model, at least, to a certain degree. For instance, the collaborative aspect is captured via the information attribute *location*. Risk analysis is covered by the RMIAS to the degree which is required for the purposes

of this model as discussed in the previous chapter. The importance of the human-factor is explicitly outlined in the RMIAS by distinguishing a whole category of human-oriented security countermeasures. Furthermore, the need to take into account the human factor during all stages of the security development life cycle, and not only at the stage of system design, is acknowledged in the RMIAS. The comment regarding business goals concerns the understanding of the place and role of IAS in an organisation, rather than the structure of the IAS domain. In agreement with the need for alignment of security goals with business objectives, the narrative of the RMIAS also states that IAS does not exists for its own sake and is only used by an organisation in order to achieve its overall goals. Echoing this, the role of IAS as a business enabler is also discussed in our earlier publication [6].

In question 9, twenty-four respondents stated that there are no elements in the RMIAS that are not relevant to the IAS domain. Only two respondents expressed concern about the relevance of several security goals within the IAS-octave providing the following comments: (1) "*Privacy and Auditability could be argued. (Good you have included them anyway.)*" and (2) "*I think the further subdivision of the core security goals (integrity, availability and confidentiality) may assist people in understanding what the element entail, but may not add anything as separate goals in their own right.*"

5.5. Systematic Power of the RMIAS

The RMIAS systematises the IAS domain by distinguishing four key dimensions and, then, elaborating each dimension in depth. The RMIAS brings together these four dimensions and explains the correlations between them.

Question 10 in the questionnaire attends to the systematic power of the RMIAS and was worded as follows: Does the model organise elements of the IAS domain and relationships between them in a structured, systematic way?

Answering this question, twenty-two respondents acknowledged that the RMIAS presents the IAS domain is a systematic way. One respondent was not sure about the answer. Three respondents expressed reservations regarding the systematic power of the RMIAS with one of them saying "*I am not convinced it does. There are a number of reasons for my view, not least of which is the lack of "systemic understanding" among managers. I fear the arrows in the model will be interpreted as a time dependency, rather than a logical interdependency.*".

5.6. Explanatory Power of the RMIAS

The RMIAS may assist with the elimination of omissions and contradictions in ISPDs. It helps to identify overlooked threats, i.e. predict possible security violations and search for required countermeasures. Due to the fact that the RMIAS is more complete and accurate than the other models it may be hypothesised that the RMIAS may explain and indicate more security issues. The following example confirms this hypothesis. If accountability and

legal security countermeasures are not included in a model (our analysis confirms that none of the examined models includes accountability, and legal and organisational security countermeasures at the same time [3]), then the model could not assist with explaining security violations that stem out of the absence of legal measures that help to keep misusers accountable for their actions. E.g. a bank logs an unauthorised access of an employee to confidential account information of bank's customers. Then, the bank attempts to sue the employee for the information misuse. The access log (e.g. the evidence received by means of a technical security countermeasure) may be insufficient in a legal mitigation, because the prosecution of an employee also depends on the clarity of the bank policies regarding information access and on the knowledge of the employee regarding his/her access rights which may be confirmed by attended security training and by a signed information access policy (i.e. organisational, human-oriented and legal countermeasures) [45].

Question 11, which was worded as "Might the Model assist with explaining (tracing back) and predicting issues related to IAS?", was intended to capture the opinion of the respondent with regard to the explanatory power of the RMIAS.

Answering this question, ten respondents clearly saw the RMIAS as a tool that may help to explain IAS issues: "*I think your model will assist in predicting issues and tracing them back thanks to the goals, which occupy the third dimension of your model*" and "*Yes, using the model you would be able to trace back logically and demonstrate how an element of InfoSec had been missed.*"

Seven respondents found that the RMIAS has explanatory power, but only with some limitations. For example, it may help only to explain security events, but not to predict them. One of the comments was as follows: "*Security audit based on the model may give some level of traceability. The model could be used retrospectively, to trace back security incidents, to see where things went wrong. But to predict will be very difficult.*" Six respondents were not sure about the ability of the RMIAS with helping to predict/trace back security issues. Three respondents answered in the negative to question 11.

5.7. Reliability of the RMIAS

The reliability of the RMIAS is evaluated through the examination of two aspects.

First is the assurance that the RMIAS is applicable for the majority of organisations irrespectively of size and domain (wide applicability). The RMIAS draws upon a broad spectrum of IAS literature which synthesises the IAS practice of many organisations. Therefore, the applicability of the RMIAS to the majority of organisations is anticipated. Further, the flexibility and adjustability of the RMIAS makes it widely applicable. The model outlines a template which may be adjusted to suit a specific organisation. During the workshops the applicability of the RMIAS in the context of an SME is empirically tested. The applicability of the RMIAS in the context of a large enterprise is practically demonstrated by the case

study. The outcomes of the workshops and case study are discussed in Sections 6 and 7 respectively. Second is the assurance that the RMIAS leads to similar understanding when applied by different users. This aspect is tested via the workshops as well.

Question 12 gauges the reliability of the RMIAS:

- Question 12 - In your opinion, would the model be applicable for the majority of business organisations? Are there any industries or types of organisations where the model would not be applicable (explain your opinion)?

Answering question 12, sixteen respondents consider the RMIAS to be applicable to any organisation without exceptions (two respondents specifically pointed to its applicability in the military and healthcare environments). In the opinion of five respondents the RMIAS had limited applicability. One respondent had concern about the applicability of security goals and their interpretation within the healthcare domain. One respondent considers the RMIAS to be more suitable for smaller businesses with less resources as it may be hard for large scale organisations to use the model, while another, on the contrary, stated that the RMIAS is not applicable to SMEs.

5.8. Validity of the RMIAS

The RMIAS provides guidance for the development of an ISPD (Section 3). Thus, the validity of the RMIAS is tested by evaluating whether the RMIAS facilitates the development of an ISPD via the workshops and case study as considered in Sections 6 and 7.

Question 13 in the questionnaire captured the opinion of the respondents with regard to the validity of the RMIAS. The question was formulated as follows: "Would the methodology embodied into the model lead to valid results (e.g. comprehensive security policies, correct prediction of InfoSec issues, meaningful tracing back of security breaches)?"

Eleven respondents confirmed the ability of the RMIAS to produce valid results without providing additional comments. Five respondents suggested that the use of the model might lead to valid results and additionally commented that (1) the validity of the results may be strongly influenced by the knowledge and understanding of people applying the model, (2) for producing valid results there must be a risk analysis methodology aligned with the model, and (3) the used of the model may be labour intensiveness. The authors agree with the comments provided by the interviewees and discuss these comments later on in this paper. Two respondents answered in the negative to question 13. Eight respondents were not able, based on the provided information, to judge the ability of the RMIAS to render valid results. Overall, 16 respondents (62%) evaluated the validity of the RMIAS positively, with 5 out of them noting additional influences and needs that must be taken into account.

As the RMIAS provides a framework for structuring thinking about IAS, the results produced using the model will inevitably be affected by the characteristics of an individual applying it. The RMIAS, at least at this stage, was intended as an automated decision

support tool that would completely exclude the need for expertise and produce valid results irrespectively.

Answering the concern of the interviewees regarding the labour intensiveness, it must be acknowledged that the application of the RMIAS may potentially produce an extensive list of security statement. However, the purpose of the RMIAS is to helps to identify a *complete* list of situations or scenarios where information may need protection. This inevitably will lead to a large amount of information that must be processed. It may be considered in future how the development of a security policy document using the RMIAS may be simplified and optimised without compromising on the completeness or scope of a security policy document. Also the amount of data generated using the RMIAS will depend on the complexity of business and other organisation specifics. It is assumed that the larger organisations and organisations for whom the protection of information is more critical have more resources available to assist with the generation of security policy and must allocated them more readily.

The uncertainty of a large number of respondents regarding the questioned ability of the RMIAS may be explained by the insufficient amount of information they had to make a judgement about it. The intention of the interviews was to capture the initial judgement of the experts regarding the validity of the RMIAS. It was not feasible to present to all experts interview the examples of the use of the RMIAS in several case studies. In order to further test the validity of the RMIAS, the workshops and case study were undertaken where the participants had a chance to use the RMIAS in practice. The results of the workshops and a case study are discussed in the subsequent sections.

5.9. Fruitfulness of the RMIAS

Fruitfulness is a desirable characteristics of a conceptual model to suggest research problems and hypothesis to be verified [38, 7].

The RMIAS, in conjunction with the examination of the literature, may assist in a search for research problems. It is described below how it may be done. Using the information taxonomy of the RMIAS, the category of information is identified. A security goal is specified for this category. The RMIAS suggests to search for a security countermeasure that may help to ensure the goal for the category of information. If the literature review shows that such countermeasure is not present (or the existing countermeasure is not efficient), then the need for a new countermeasure is detected. The RMIAS also points to a need to explore whether there are methods to cover security goals, countermeasures, and the information taxonomy at different stages of the security development life cycle.

Two questions in the interviews were aimed at the evaluation of the fruitfulness of the RMIAS:

- Question 14 - Does the model provide a convenient structure for framing the existing research? How would you position your area of research/practice using the model?

- Question 15 - Could the model assist with pointing out the gaps in the existing research/practice?

Only eight respondents had background in research to enable them to answer these questions. In question 14, while two respondents were not sure about the answer, six agreed that the RMIAS provides a convenient structure for framing research and were able to pinpoint the place of their own research topic within the model. In question 15, seven out of eight respondents agreed that the RMIAS may point out at the gaps in research *...due to the way the model splits out the different dimensions of InfoSec and further splits these down prompting thought on each individual aspect of information security* and one respondent was not sure about the answer. In both questions the vast majority of the interviews has confirmed the fruitfulness of the RMIAS.

In this project, we had only a small number of participants to test the fruitfulness of the RMIAS. Hence, the conclusion we make about the fruitfulness of the RMIAS is only suggested by our results, and further interviews and case-studies are needed in the future to fully corroborate our conclusion. We also deemed it incorrect to exclude fruitfulness from the evaluation due to this reason. Randomly excluding criteria from the evaluation would hinder the comprehensiveness of the evaluation, though the evaluation result regarding with this criterion must be taken with greater caution due to the lower number of participants.

6. Evaluation Workshops

Three evaluation workshops were conducted. The first workshop was with the group of MSc students specialising in Information Security & Privacy at the School of Computer Science & Informatics, Cardiff University. The group consisted of students who came straight after receiving BSc degree and did not have any practical experience. This group was a suitable audience for testing the simplicity, explanatory and systematic powers of the RMIAS with the audience lacking the extensive experience in the IAS domain. However, the group was familiar with the ISO/IEC 27000 series of standards and, prior to the workshop, developed a security policy document for another case study using ISO/IEC 27001 and ISO/IEC 27002 standards as guidance. The second workshops was with the group of MSc students specialising in Cyber Defence and Information Assurance at Cranfield University. This group among 13 participants included 10 mature students with experience in the IAS domain varying from 1 to 20 years. The third workshop was with the group of security professionals and included an IT security expert, records manager, the head and a manager of an InfoSec program at a large higher education institution.

Each group was given a one-hour presentation of the RMIAS followed by a one-hour workshop where the participants applied the RMIAS to the case study of Translate. The case study outlines the current security arrangements of Translate, the problems which the

company was facing, the changes the business went through recently as well as the details of the information classification scheme of the company. The participants were asked, while working in a team of 2-4 people, to develop an Information Security Policy Document (ISPD) for Translate using the RMIAS. The case study and the task as they were given to the participants are presented in [3, App. 5].

During two workshops, 6 teams were formed. The participants were allowed to refer to ISO/IEC 27001 and ISO/IEC 27002 standards. The teams followed the methodology for the derivation of an ISPD described in Sections 3. First, the teams produced tables in MS Excel which they populated with the combinations of four information attributes and security goals. Then, the groups discussed each combination and attempted to work out a scenario for each combination and make a judgement on whether a scenario posses any threats to *Translate*. If they answered positively on the last question then the teams identified security countermeasures that contribute to the achievement of the security goal for the category of information under consideration. The teams developed between 3 to 8 security policy statements each. The workshops reproduced how the RMIAS must be utilised in real cases with the only exception that the risk analysis was not conducted following any particular methodology, but rather left for the judgement of the participants. At the end of the workshops, the participants provided feedback.

Since the RMIAS only provides a template to be filled in with policies, the quality of policy statements strongly depends on the knowledge and experience of its developer(s) and on information they have at hand, as was also pointed out at by the experts interviewed (Section 5.8). The viability and compliance to reality of the security statements developed by the teams were assessed by the authors and, then, confirmed with the IAS expert who has security experience both in academia and industry, and was present at the workshops as an observer. The actual ISPD statements developed by the participants of the workshops may be found in [3, App. 9]. It was concluded that all statements are valid and comply with reality.

The purpose of the workshops was to observe how well the RMIAS is comprehended by the participants with the different levels of expertise in IAS and whether the participants are able to use the RMIAS while working in a team, and to gather the feedback of the participants on the use of the RMIAS. Further, we present outline our observations and the feedback on the use of the RMIAS provided by the participants.

The workshops confirmed that the majority of the participants managed to get a solid understanding of the RMIAS and how a policy document may be developed using the RMIAS. There was only one team of three MSc students who significantly struggled with the task. However, after additional help the team managed to produce 3 valid policy statements. Other teams worked independently and only in several cases called for minor clarifications.

The final feedback of the participants indicates that the participants appreciate that the RMIAS helps with profiling information - "*the complete registry of all information organisa-*

tion has is good because nothing is omitted from a policy document". Each team was able to identify the scenario in which a specific category of information needed protection from threats referred to by a specific security goal.

The IAS-octave was found by the participants useful. According to the feedback of the teams "*the IAS-octave covers all possible issues with information*". The participants also appreciated the help the RMIAS provides with the identification of scenarios in which information needs protection.

There was only one MSc student who struggled with the concept of security goal. The student suggested to include in the final table, along with the name of a security goal, more detailed description of attacks and threats to which the goal refers to. This approach is not optimal, as it leads to the duplication of information. However, it is suggested when presenting the RMIAS in future and, the IAS-octave specifically, to provide an audience with more examples of threats and attacks which pose threats to each security goal.

According to the comments of the participants of the workshops, using the RMIAS it was easier to see how an ISPD must change (i.e. which security statements to be included, excluded or corrected) when a change in an organisation which affected any of the elements of the RMIAS took place. The participants also suggested that the RMIAS may serve as a tool for benchmarking of the ISPDs of different organisations which may be specifically fruitful in the context of a collaborative environment and cross-organisational information sharing. Thus, the RMIAS may help to see the differences between the document classification as well as location categorisation schemes of different organisations. It may also highlight the difference of the approaches to IAS by comparing security goals (and their definitions) and the types of security countermeasures which are recognised and exploited by different organisations. Furthermore, the RMIAS may help to compare which security countermeasures are used by different organisations in similar situations. This may be helpful when ensuring the compliance of the security policies of one organisations with the policies of another one and in certification.

The group of MSc students, who previously developed an ISPD based on the ISO/IEC 27001 and ISO/IEC 27002, was able to compare the process of the development of an ISPD guided solely by the ISO/IEC standards and the same process guided by the RMIAS in conjunction with the ISO/IEC standards. The feedback of this group indicated that the use of the RMIAS aids in judging the completeness of an ISPD. The RMIAS helps to ensure that all possible problematic situations and all categories of information are covered by an ISPD, while working with the ISO/IEC standards only, there was no way to make any judgement regarding the completeness of an ISPD. One of the teams also noted the benefits of the explicit declaration of knowledge as one of the forms of information which needs protection. The team said that discussing how different security goals may be achieved for knowledge or verbal information greatly assists with the identification of security violations scenarios and, consequently, security statements covering knowledge protection, which would unlikely

emerge during the work on an ISPD otherwise.

The group of practitioners who participated in the third workshop indicated that it is always challenging to reflect all possible threat situations in an ISPD as there is no framework based on which one can gauge whether everything is dealt with or not. The group agreed that the RMIAS provides useful guidance on how the complete set of such situations may be determined. The group also agreed that the IAS-octave certainly prompts one to consider more threat scenarios than, for example, the CIA-triad. Although this group originally voiced a concern about the overlap between some security goals, after working on the Translate case study the group agreed that the explicit acknowledgement of all eight goals of the IAS-octave was helpful, specifically, for the audience inexperienced in IAS. If any of the goals was omitted from the model, then an organisation relies purely on the knowledge and expertise of an expert developing an ISPD to identify and tackle threats to information which the omitted goal covers.

The group of participants from Cranfield University also suggested that the RMIAS may serve as a tool for security audit and benchmarking by large and small organisations. The participant, who had experience in the field of IAS consultancy also predicted that the RMIAS may serve as a consultancy framework.

7. Case Study

This is a case study of an executive non-departmental public body based in the UK. The name of the organisation may not be revealed due to the non-disclosure agreement. Further in the text, the organisation is referred to as the Agency. The Agency has multiple offices across the UK and employs over 1000 people. While in the workshops the RMIAS was exploited to produce an ISPD from scratch, in this case study the RMIAS was employed to structure and organise the existing ISPDs.

The Agency provided the authors with four ISPDs: (1) Agency data security standard (8 pages); (2) Classifying and handling sensitive information policy (25 pages); (3) Sending, transferring and storing data policy (3 pages); and (4) Protective security policy (3 pages). The documents were initially analysed to identify which elements of the RMIAS are present. The examination of documents confirmed that all elements of the RMIAS were present in the policies. The precise values of the elements were extracted and are stated below.

The organisation uses the UK government sensitivity classification and marking scheme: Top Secret, Secret, Confidential, Restricted, Protect and Unclassified [46][7].

[7]The government classification scheme was changed in 2013 [47] after this case study was performed.

The following locations are listed in the examined policy documents: the Agency offices; the supporting IT company; the third parties storing information on behalf of the Agency; home environment (employees who work from home); and locations other than the above. It was agreed to categorise the locations as suggested in Section 3 into controlled, uncontrolled and partially controlled.

The state of information is acknowledged in the analysed documents. It was specifically noted that countermeasures were specified for the protection of information at the stages of creating and destruction as well as at the stages of processing, transmission and storage. This further confirmed the correctness of the incorporation of these stages into the information taxonomy of the RMIAS.

Security countermeasures of all four types, namely legal, technical, organisational and human-oriented were encountered in the analysed policies. As it was anticipated, the analysed documents stated only the CIA-triad (confidentiality, integrity and availability) as the security goals to be achieved.

After all elements of the RMIAS were identified, the RMIAS was adjusted with the values specific to the Agency (e.g. information sensitivity and location classification). The IAS-octave replaced the CIA-triad and was used in the analysis.

Using the values of information sensitivity and location specific to the Agency, a table was created as described in Section 3. The table was populated with all possible combinations of the values of such parameters as information form, information sensitivity, information location, information state and security goal.

Then each security statement in the analysed documents was examined and assigned in to the appropriate combination of the information category and security goal (i.e. the column Security Countermeasure of the table in a specific row in the table was populated with the description of this security countermeasure).

For example, when the statement "Documents marked *Confidential* may be taken home only with a written approval of a designated person" was examined it was assigned to the row with the following characteristics: information form - paper, sensitivity - *Confidential*, location - partially controlled, state - transmission, security goal - confidentiality.

In the final table the rows were flagged which contained the combinations of information categories and security goals for which no security controls were specified in the analysed documents (i.e. the last column of the final table was empty for that row). These rows identify the situations which were not covered by the examined ISPDs.

The final table was presented to and discussed with the Information Security Officer of the Agency. Two meetings took place. At the first meeting the RMIAS was presented and initial information was received from the Agency. The exchange of email helped to identify the missing information. At the second meeting the finalised table was presented to the Agency, and feedback was received. Both meetings were run informally and comments were provided

in a free form. The feedback received is discussed below.

The Agency had no other model of IAS in place and willingly adopted the RMIAS. According to the Agency, the RMIAS "*makes perfect sense*" in the context of the Agency and provides a way of approaching security in a more structured way.

At the first meeting, the Agency saw the IAS-octave as the main advantage of the RMIAS. Since the existing policies of the Agency were confined to the CIA-triad, the Agency anticipated that considering the wider spectrum of threats beyond the CIA-triad may help to improve the policy documents and identify the threats that were potentially overlooked. The Agency also positively evaluated the segregation of legal security countermeasures. A discussion took place on whether it is legitimate to consider law as a security countermeasure and the agreement was reached that it is, since an organisation may refer to law in order to protect its information.

At the second meeting, it was agreed by the Agency that the information taxonomy and security goals dimensions of the RMIAS provide a basis for a good coverage of all potential situations in which information needs protection ("misuse cases"). It was confirmed that by using the RMIAS, more potentially dangerous cases where information needs protection may be identified.

The policy statements of the Agency were spread over a number of documents developed and updated by a number of employees at different time. Therefore, the fact that the RMIAS helps to organise the policies extracted from various policy documents in a form which is easy to manage and analyse, was seen as one of the major positive outcomes of the use of the RMIAS.

The analysis and structuring of the Agency's security policies enabled the Agency to see the range of the countermeasures of different types declared in various documents and applicable to the same category of information for achieving the same security goal. This provided a basis for a cost-effectiveness and efficiency analysis, and for the improvements of the ISPDs (i.e. duplicated countermeasures may be removed or the most cost-effective alternative may be chosen). The Agency also expressed interest in a software system which will be based on the RMIAS and will provide security recommendations for particular situations and particular categories of documents.

The case study confirmed that the RMIAS (1) helps to organise, in a manageable form, security policies spread over multiple documents, (2) permits the tracing of the contradictory security policy statements, and, most importantly, (3) facilitates the identification of omissions in security policies.

8. Discussion

The results of the interviews are summarised in Figure 3. The y-axis shows the questions in the interviews and the evaluation criteria they correspond to, and the x-axis shows the

number of the responses. It must be noted here that the interviewees did not give answers such as "Yes" or "No", but provided extensive comments which were then analysed by the authors and grouped into various categories. It was not always possible to categorise answers in to a binary category of "Yes" or "No", and for some questions we introduced additional categories such as "Yes, with some limitations", for example. (The detailed discussion of the answers are presented in the preceding Sections 5.2-5.9.) This summary analysis was done in order to simplify the presentation and analysis of the results for the reader.

Among all examined criteria, the accuracy of the interrelationships between the dimensions (arrows) of the RMIAS received the lowest support of only 14 respondents (54%), while the accuracy of the elements received the support of 18 respondents (69%). Hence, in the future enhanced versions of the RMIAS, more attention must be paid to the description and clarity of the interrelationships between the dimensions as this proved to be one of the most challenging aspects of the model. The relevance of the elements of the RMIAS received the highest support with 24 respondents (92%) confirming it. The simplicity of the elements was supported by 22 (85%). The completeness of the RMIAS was endorsed by 18 (69%) respondents. Overall, more than 50% of the interviewees endorsed the RMIAS for simplicity, accuracy, covered scope, systematic power, reliability and validity.

The participants of the workshops, even those who had limited experience in IAS, were able to exploit the RMIAS for the development of an ISPD after only a one-hour presentation of the model. This also supports the hypothesis that the RMIAS represents the essence of the IAS domain at a level which is easy to comprehend even by a novice audience. As was noted by the participants of the workshops, the RMIAS is a more effective way of describing IAS than as a set of definitions or rules. Many participants stated that with the RMIAS they acquired a more comprehensive vision of IAS (one participant even described it as "*eye-opening*"). Many participants were able to pinpoint the place of their personal topic of interest in IAS in the overall picture of the domain.

During the presentations and workshops, the IAS-octave usually sparked intensive discussions. The participants challenged the meaning of and the differences between security goals. In these discussions, the IAS-octave was acknowledged to be more comprehensive than other sets of goals (e.g. the CIA-triad) and to cover all known to the participants threats to information. No additional security goals were suggested during the interviews or workshops.

The evaluation results confirm the reliability of the RMIAS in two ways. First, the results of the interviews corroborate the applicability of the RMIAS for the majority of organisations. More than 50% of the experts anticipate no restrictions to the fitness of the RMIAS in the context of any specific domain (Section 5.7 - question 12 in Figure 3). Furthermore, the case study demonstrated how a large-scale organisation may avail of the RMIAS, while in the workshops the RMIAS was successfully applied in the context of an SME. Second, the workshops, demonstrated that the RMIAS leads to the congruous understanding of the IAS

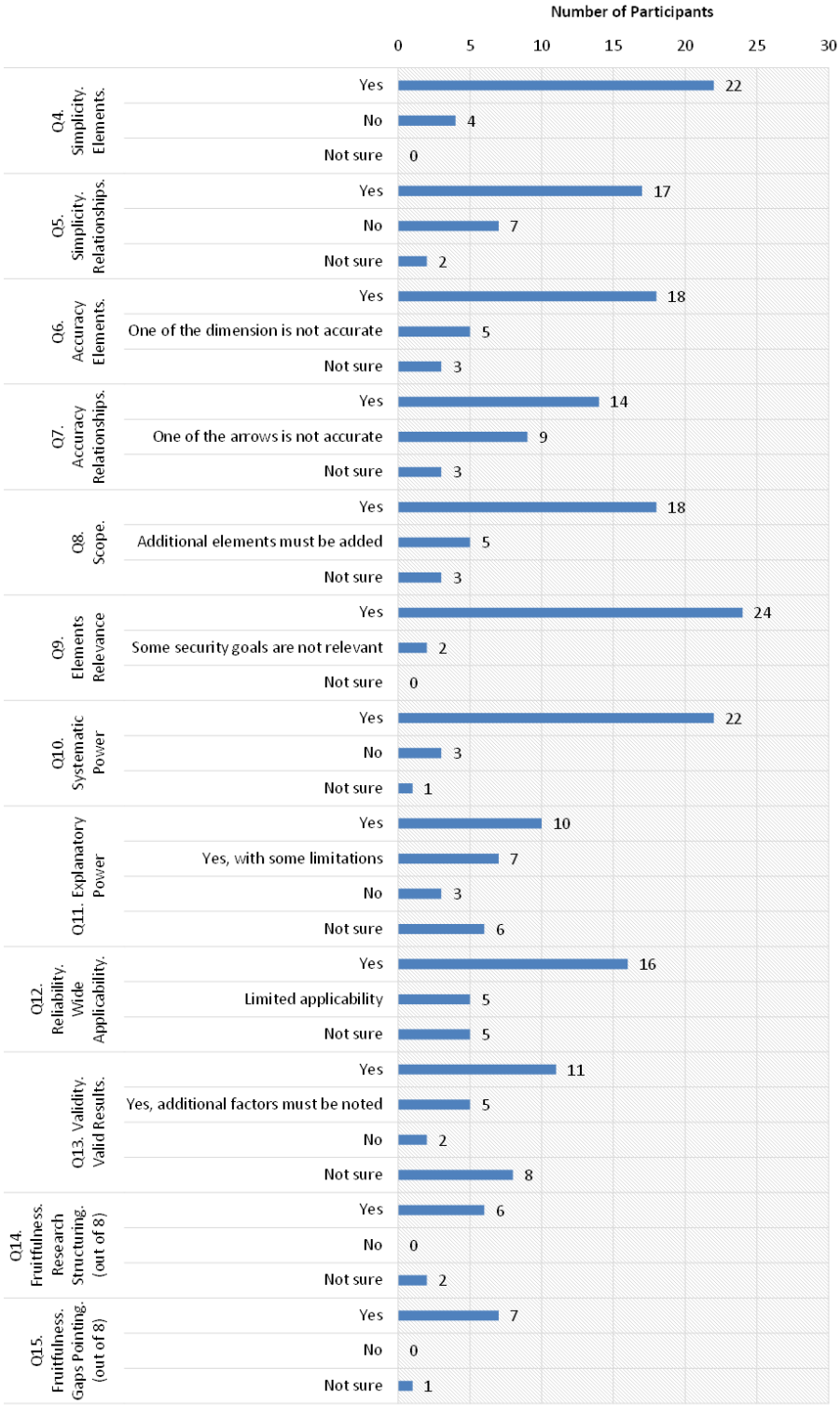

Figure 3: Summary of the Interview Answers

domain when applied by different users. The participants of the workshops were able to work as a cohort to produce security policy statements using the RMIAS.

The analytical evaluation of the RMIAS as well as the interviews with the IAS domain experts did not explicitly cover the cognitive effectiveness of the visual appearance of the RMIAS. However, during the workshop at Cranfield and Cardiff Universities, while providing the feedback on the RMIAS, the participants of the workshops explicitly highlighted the clarity and cognitive effectiveness of the RMIAS as one of the strengths of the model. This work does not make any strong claims with regard to the cognitive effectiveness of the RMIAS because it was not the primary focus of this research project. Nevertheless, it is worth pointing out that to the best of the authors' knowledge, the RMIAS is the first model which provides the design rationale for its visual appearance. However, further work regarding the visual appearance of the RMIAS and its evaluation is required.

The workshops and case study which tested the reliability and validity of the RMIAS demonstrated that the RMIAS (a) is applicable to large and small organisations of different domains, (b) leads to similar understanding of the IAS domain when used by different users, and (c) helps to render a valid ISPD and structure it in a useful way. The conclusion regarding acquiring a similar understanding of the domain is based on the observations that (1) during the presentations and workshops, the participants asked meaningful questions, i.e. they all understood the model in a way it was intended, (2) both the novices and the experts in the domain were able to understand the model and use it as intended; (3) the participants were able to use the model while working in a team, i.e. within a team there was an agreed-upon understanding of the domain and its main concepts, and of the way how it must be applied to a specific case, and (4) all six teams of the workshops' participants developed meaningful security policy statements which all had a resemblant format, i.e. the understanding of the RMIAS and the way it must be used for the development of an ISPD for a specific case was also coherent among the teams.

There are a number of limitations to the evaluation process which are outlined below. The evaluation was conducted by the team including the authors of the RMIAS who were inevitably biased. To deal with this, we used a well defined evaluation methodology and through documentation of the process as well as of the interviews and feedback. The results of interviews may be affected by many factors [43] including the command of language and background of both interviewee and interviewer, the inconsistent interpretation of terminology, the lack of motivation, etc. In this research project, although the participants were not financially or in any other way motivated to participate in the evaluation process, they demonstrated, as mentioned above, a profound interest in the RMIAS, and readily and actively participated in its evaluation.

It may be debated how well the MSc students, who were involved in the evaluation, stand proxy for a novice audience. Although the group at Cardiff University had no practical

experience in IAS, they already were taught several modules on IAS by the time the evaluation took place. Hence, although they knowledge was limited, they were not complete novices to IAS.

Finally, there were a number of critical comments regarding the RMIAS received during the interviewing process. All the comments are discussed in the proceeding sections. In this paper, the RMIAS is presented in the same form as it was presented to the experts interviewed. The RMIAS was not modified according to the comments and this will be done as a part of future work.

9. Conclusions

The evaluation presented in the paper at hand verifies the hypothesis declared in Section 1 and confirms that (1) the RMIAS provides more complete and accurate representation of the IAS domain, than the existing conceptual models of the IAS domain; (2) the RMIAS reflects the IAS domain as it is understood by the majority of the experts interviewed; and (3) represents the domain in the form accessible by the experts with different backgrounds and with the different levels of experience in IAS. As such, the RMIAS is a suitable cognitive model and a basis for building a congruent understanding of the IAS domain in a multidisciplinary team of security and non-security experts.

The evaluation of conceptual and reference models is a challenging task and is a research topic attracting the close attention of research community [7, 1, 48]. The multifaceted and multi-criteria evaluation carried out in this research project to verify the quality of the RMIAS provides a rigorous example of an evaluation process. This evaluation process used is justified, transparent, and based on a well-established framework. This process may arm other researchers, reference model developers and evaluators. The evaluation route pursued combines the analytical and empirical evaluation methods, thus dealing with the drawbacks of separate methods. The evaluation conducted relied strongly on the involvement of people other than the developer(s) ensuring the objectiveness of the evaluation results.

Summing up, the contribution of this paper is three-fold: (1) a review of the conceptual models of the IAS domain in terms of their evaluation; (2) the development and implementation of a procedure for a multifaceted, multi-criteria evaluation of a reference model, and (3) the evaluation of the RMIAS and the corroboration of its validity.

References

[1] D. Moody, "Theoretical and practical issues in evaluating the quality of conceptual models: Current state and future directions," *Data Knowl. Eng.*, vol. 55(3), 2005, pp. 243-276.

[2] Cherdantseva Y. and Hilton J. "A Reference Model of Information Assurance & Security," SecOnt 2013 workshop in conjunction with the 8th International Conference on Availability, Reliability and Security (ARES) 2013, University of Regensburg, Germany. September 2nd - 6th, 2013. IEEE Proceedings.

[3] Y. Cherdantseva, Secure*BPMN - a graphical extension for BPMN 2.0 based on the reference model of Information Assurance & Security. PhD Thesis. Cardiff, UK. 2015.

[4] A. Jede and F. Teuteberg, "Towards a document-driven approach for designing reference models: From a conceptual process model to its application." Journal of Systems and Software 111 (2016): 254-269.

[5] OASIS, "Reference Model for Service Oriented Architecture", OASIS Standard version 1.0 , 12 October 2006.

[6] Y. Cherdantseva and J. Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," In: *Organizational, Legal, and Technological Dimensions of Information System Administrator*. F. Almeida and I. Portela, Eds. IGI Global Publishing, 2013, pp. 167-198.

[7] K. Järvelin and T. Wilson, "On conceptual models for information seeking and retrieval research", *Information Research*, 9(1), 2003, pp. 163.

[8] P. Fettke and P. Loos, "Perspectives on Reference Modeling," in P. Fettke & P. Loos (eds.) *Reference Modeling for Business Systems Analysis*, Idea Group, 2007, pp. 1-20.

[9] A. Ekelhart, S. Fenz, M. Klemen, E. Weippl, "Security Ontology: Simulating Threats to Corporate Assets," In: Information Systems Security, LNCS, A. Bagchi, V. Atluri, Eds., vol. 4332, Springer, 2006, pp. 249-259.

[10] ISACA, "An Introduction to the Business Model for Information Security," 2009.

[11] ISO/IEC 27002:2005, "Information technology - Security techniques - Code of practice for information security management".

[12] J. McCumber, "Information Systems Security: A Comprehensive Model," In Proceeding of the 14th National Computer Security Conference, NIST, Baltimore, MD, October, 1991.

[13] D. Pipkin, *Information Security: Protecting the global enterprise.* Hewlett-Packard Company, 2000.

[14] D.Lacey, *Managing the Human factor in information security.* J. Wiley and Sons Ltd., 2009.

[15] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2001.

[16] D. Parker. "Fighting Computer Crime." NY: J. Wiley and Sons, 1998.

[17] Neumann P. "Computer-Related Risks." ACM Press/Addison Wesley. 1995.

[18] M. Salnitri, F. Dalpiaz, P. Giorgini, "Modeling and verifying security policies in business processes," *Enterprise, Business-Process and Information Systems Modeling*. Springer Berlin Heidelberg, 2014, pp. 200-214.

[19] C. Blanco, J. Lasheras, E. Fernández-Medina, R. Valencia-García, and A. Toval, "Basis for an integrated security ontology according to a systematic review of existing proposals," *Computer Standards & Interfaces*, 33(4), 2011, pp. 372-388.

[20] M. Sabbari and H. Alipour, "A Security Model and its Strategies for Web Services," *International Journal of Computer Applications*, 36.10, 2011.

[21] Oracle. Information Security: A conceptual architecture approach. April 2011

[22] S. Ransbotham and S. Mitra, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research*, 20(1), 2009, pp.121-139.

[23] Robert E. Slavin, Best-Evidence Synthesis: An Alternative to Meta-Analytic and Traditional Reviews, Educational Researcher, Vol. 15, No. 9 (Nov., 1986), pp. 5-11.

[24] Vermeulen, Clive, and Rossouw Von Solms. "The information security management toolbox - taking the pain out of security management." *Information Management & Computer Security*, 10(3), 2002, pp. 119-125.

[25] K. Kumar, "Information Security Management for Governments", ISACA Journal, 4, 2011.

[26] W. Maconachy, C. Schou, D. Ragsdale, D. Welch, "A Model for Information Assurance: An Integrated Approach," In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, U.S. Military Academy, West Point, NY, 5-6 June, 2001.

[27] D. Trček, "An integral framework for information systems security management." *Computers & Security*, 22(4), 2003, pp. 337-360.

[28] R. Saint-Germain, "Information security management best practice based on ISO/IEC 17799," *Information Management Journal*, 39(4), 2005, pp. 60-66.

[29] M. Dark, N. Harter, L. Morales, M. Garcia, "An information security ethics education model," *Journal of Computing Sciences in Colleges*, 23(6), 2008, pp. 82-88.

[30] W. Al-Hamdani, "Non-risk assessment information security assurance model," in InfoSecCD '09, Information Security Curriculum Development Conference, Kennesaw, GA, USA, 2009.

[31] X. Lu, "Information assurance conception model and applications for largescale information systems," Signal Processing, 2006 8th International Conference on., Vol. 4. IEEE, 2006.

[32] J. Saltzer and M. Schroeder, "The protection of information in computer systems", Proceedings of the IEEE 63 (9), 1975, pp. 1278-1308.

[33] E. Jonsson, "Towards an integrated conceptual model of security and dependability," Availability, Reliability and Security, The First International Conference on. IEEE, 2006, p. 8.

[34] D. Parker, "Our Excessively Simplistic Information Security Model and How to Fix It", *ISSA Journal*, July 2010, pp. 12-21.

[35] D. Moody, "The method evaluation model: a theoretical model for validating information systems design methods," ECIS 2003 Proceedings, ECIS. 2003. pp. 79.

[36] SANS. Information Security Policy - A Development Guide for Large and Small Companies. SANS Institute. 2007.

[37] M. Whitman and H. Mattord, *Principles of Information Security*, 4th edition, Course Technology, Cengage Learning, 2012.

[38] S. Alter, "Defining information systems as work systems: implications for the IS field," *European Journal of Information Systems*, 17(5), 2008, pp. 448-469.

[39] T. Wahl, G. Sindre, "An analytical evaluation of BPMN using a semiotic quality framework," *Advanced topics in database research*, vol. 5, 2006, p. 94.

[40] S. Gopalakrishnan and G. Sindre. Analytical Evaluation of Notational Adaptations to Capture Location of Activities in Process Models. Technical report M3W-1, Department of Computer and Information Science Norwegian University of Science and Technology, August 2011.

[41] D. Moody, "The method evaluation model: a theoretical model for validating information systems design methods," . In *ECIS 2003 Proceedings*, 2003, p. 79.

[42] N. Genon, P. Heymans, D. Amyot, "Analysing the cognitive effectiveness of the BPMN 2.0 visual notation," *Software Language Engineering*, Springer Berlin Heidelberg, 2011, pp. 377-396.

[43] M. Mayers and M. Newman, "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization*, 17, 2007, pp. 2-26.

[44] D. Moody, "The "Physics" of notations: Toward a scientific basis for constructing visual notations in software engineering," *Software Engineering*, IEEE Transactions on, 35(6), 2009, pp. 756-779.

[45] R v Bow Street Magistrates Court and Allison (AP) Ex parte Government of the United States of America (Allison). 2 AC 216. 1999.

[46] HMG. HMG Security policy framework. 1 May 2010.

[47] Cabinet Office. Government Security Classifications. Version 1.0. April 2014.

[48] U. Frank, "Evaluation of Reference Models," in P. Fettke & P. Loos (eds.) *Reference Modeling for Business Systems Analysis*, Idea Group, 2007.